(19) JAPANESE PATENT OFFICE

Reference 1

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11004407 A**

(43) Date of publication of application: **06.01.99**

(51) Int. Cl **H04N 5/91**
H04H 1/00
H04L 9/08
H04N 7/167

(21) Application number: **09156312**

(22) Date of filing: **13.06.97**

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

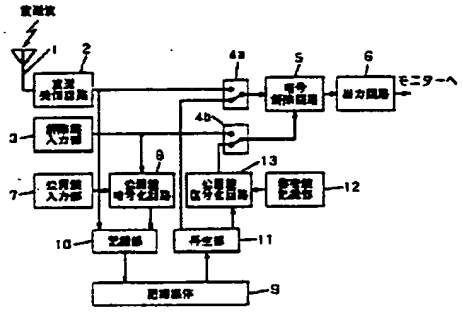
(72) Inventor: **MAEDA TAKIO**

(54) **BROADCAST SIGNAL RECORDING AND REPRODUCING DEVICE**

(57) Abstract

PROBLEM TO BE SOLVED: To provide a device by which only an imposed viewer reproduces a broadcast signal by entering a decode key to decode an enciphered broadcast signal, enciphering the key with a public key enciphering means, recording the broadcast signal enciphered by the public key enciphering means based on the broadcast signal onto a recording medium, decoding the enciphered broadcast signal with a decoding key decoded by the private key, reproducing and outputting the decoded signal.

SOLUTION: A received broadcast signal is recorded on a recording medium 9. A viewer uses a decoding key input section 3 to acquire a decoding key. A public key enciphering circuit 8 enciphers the acquired decoding key with the public key entered by a public key entry section 7 to record the decoding key on a recording medium 9 via a recording section 10. A reproduction section 11 reads the recording medium 9, outputs a broadcast signal to an encryption decoding circuit 5, and the enciphered decoding key is outputted to a public key decoding circuit 13. The public key decoding circuit 13 decodes the private key stored in a private key storage section 12, by using the enciphered decoding key at the public key decoding circuit 13 to output the decoded key to an encryption decoding circuit 5. It is decoded and outputted on a monitor.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－4407

(43)公開日　平成11年(1999)１月６日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｎ　5/91		Ｈ０４Ｎ　5/91	Ｐ
Ｈ０４Ｈ　1/00		Ｈ０４Ｈ　1/00	Ｆ
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ａ
Ｈ０４Ｎ　7/167			６０１Ｅ
		Ｈ０４Ｎ　7/167	Ｚ

審査請求　未請求　請求項の数３　ＯＬ　（全７頁）

(21)出願番号　特願平9－156312

(22)出願日　平成９年(1997)６月13日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　前田　多吉生
大阪府門真市大字門真1006番地　松下電器産業株式会社内

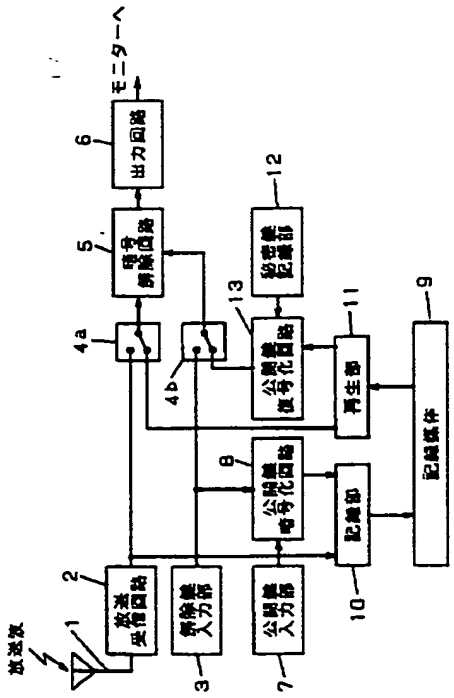
(74)代理人　弁理士　滝本　智之　（外１名）

(54)【発明の名称】　放送信号記録再生装置

(57)【要約】

【課題】　記録媒体が装置から分離可能であるとき、放送番組の著作権を保護しつつ、課金された視聴者のみが再生する機器を選択し、放送を再生することができない。

【解決手段】　暗号化された放送信号を受信する受信手段１と、前記放送信号の暗号化を解除する解除鍵を入力する解除鍵入力手段３と、前記解除鍵入力手段より入力された解除鍵を公開鍵暗号系の公開鍵により暗号化する公開鍵暗号化手段８と、前記放送信号と暗号化後の解除鍵を記録媒体に記録する記録手段９と、暗号化後に記録された前記解除鍵を前記公開鍵と対応する秘密鍵を用いて復号化する公開鍵復号化手段１３と、復号化された前記解除鍵により記録された前記放送信号の暗号化を解除する暗号解除手段５を備える。



1

【特許請求の範囲】

【請求項１】　暗号化された放送信号を受信する受信手段と、前記放送信号の暗号化を解除する解除鍵を入力する解除鍵入力手段と、前記解除鍵入力手段より入力された解除鍵を公開鍵暗号系の公開鍵により暗号化する公開鍵暗号化手段と、前記放送信号と前記公開鍵暗号化手段により暗号化された解除鍵を記録媒体に記録する記録手段と、前記記録媒体に記録された解除鍵を前記公開鍵と対応する秘密鍵を用いて復号化する公開鍵復号化手段と、復号化された解除鍵により記録された前記放送信号の暗号化を解除する暗号解除手段と、前記暗号化手段により暗号化を解除された放送信号を再生し、出力する再生・出力手段とを備えたことを特徴とする放送信号記録再生装置。

【請求項２】　公開鍵暗号化手段が複数の公開鍵を入力し、暗号化された解除鍵を複数生成する公開鍵暗号化手段であり、記録された複数の暗号化後の解除鍵の中から一つの公開鍵に対応する暗号化された解除鍵を選択し、前記公開鍵復号化手段に出力する選択手段を備えたことを特徴とする請求項１記載の放送信号記録再生装置。

【請求項３】　第１の公開鍵によって暗号化された解除鍵を前記第１の公開鍵に対応する第１の秘密鍵を用いて復号化する第１の公開鍵復号化手段と、前記第１の公開鍵復号化手段により復号化された解除鍵を前記第１の公開鍵とは別の第２の公開鍵により暗号化する公開鍵暗号化手段と、前記第２の公開鍵に対応する第２の秘密鍵により前記公開鍵暗号化手段により暗号化された解除鍵を復号化する第２の公開鍵復号化手段とを備えたことを特徴とする請求項１記載の放送信号記録再生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、放送信号を記録媒体に記録し、再生することのできる放送信号記録再生装置に関するものである。

【０００２】

【従来の発明】従来より、有料システムとするために放送信号を暗号化して、著作権を保護しているＣＡＴＶや衛星放送などがある。配信された放送信号を著作権を保護しつつ記録媒体に記録するための装置として、「特開平７－１５４３８５号公報：妨害重畳情報処理装置」等が開示されている。

【０００３】以下、著作権を保護する機能を有する妨害重畳情報処理装置の構成と動作を、図５を用いて同時に説明する。

【０００４】図５に示すように、放送信号の受信手段である放送受信回路５０２はアンテナ５０１を介して放送信号を受信する。得られた放送信号は、暗号化された信号であり、この暗号化された受信信号がそのまま再生される場合は、切換回路５０３ａを経て暗号解除回路５０４に送られる。解除鍵入力部５０５は前記暗号化された放送信号の暗号化を解除するための解除鍵を視聴者の入力、あるいは電話等の通信手段を用いて取得する。前記解除鍵入力部５０５により取得された解除鍵はスイッチ５０３ｂを経て前記暗号解除回路５０４に送られ、前記暗号解除回路５０４は暗号化された前記放送信号の暗号を解除し、出力回路５０６を通じてモニタに送り、再生する。この暗号化された受信信号が記録される場合は、記録部５０７に送られ、同時に解除鍵入力部５０５により取得した解除鍵も記録部５０７に送られ、記録媒体５０８に記録される。記録された放送信号と解除鍵は再生部５０９によりそれぞれ切換回路５０３ａ、切換回路５０３ｂを介して暗号解除回路５０４に送られる。暗号解除回路５０４は暗号化された前記放送信号の暗号を解除し、出力回路５０６を通じてモニタに送り、放送を再生する。

【０００５】なお、放送局毎、放送チャンネル毎に異なる暗号化が行われている。したがって、放送局や放送チャンネル固有の解除鍵データにより解除しない限り、視聴可能な状態には再生されない。即ち、これにより、放送信号を記録できても、専用の妨害重畳情報処理装置がない限り再生ができないため、著作権の保護が可能となる。

【０００６】

【発明が解決しようとする課題】しかしながら、上記のような従来の装置では、記録媒体が入れ替え可能であるなら、記録媒体に記録された放送信号は同じ種類の専用の処理装置であればどれでも再生が可能である。

【０００７】即ち、従来の装置を用いた有料放送システムでは、もし記録媒体が装置から取り外し可能であれば、記録媒体を課金されていない装置に接続することにより、その装置でも再生が可能となり、著作権を保護できない。したがって、著作権を保護するためには、記録媒体が装置から分離できない形の装置を用いるしか有料放送システムを構築できなかった。

【０００８】本発明は、従来の放送信号記録再生装置のこの様な課題を考慮し、放送信号を記録した記録媒体が装置から分離可能であり、有料放送システムにおいて課金された視聴者のみが記録媒体に記録された放送信号を再生できる放送信号記録再生装置を提供することを目的とする。

【０００９】

【課題を解決するための手段】請求項１記載の本発明は、暗号化された放送信号を受信する受信手段と、前記放送信号の暗号化を解除する解除鍵を入力する解除鍵入力手段と、前記解除鍵入力手段より入力された解除鍵を公開鍵暗号系の公開鍵により暗号化する公開鍵暗号化手段と、前記放送信号と前記公開鍵暗号化手段により暗号化された解除鍵を記録媒体に記録する記録手段と、前記記録媒体に記録された解除鍵を前記公開鍵と対応する秘密鍵を用いて復号化する公開鍵復号化手段と、復号化さ

れた解除鍵により記録された前記放送信号の暗号化を解除する暗号解除手段と、前記暗号化手段により暗号化を解除された放送信号を再生し、出力する再生・出力手段とを備えたことを特徴とする放送信号記録再生装置である。

【００１０】請求項２記載の本発明は、前記公開鍵暗号化手段が複数の公開鍵を入力し、暗号化された解除鍵を複数生成する公開鍵暗号化手段であり、記録された複数の暗号化後の解除鍵の中から一つの公開鍵に対応する暗号化された解除鍵を選択し、前記公開鍵復号化手段に出力する選択手段を備えたことを特徴とする請求項１記載の放送信号記録再生装置である。

【００１１】請求項３記載の本発明は、第１の公開鍵によって暗号化された解除鍵を前記第１の公開鍵に対応する第１の秘密鍵を用いて復号化する第１の公開鍵復号化手段と、前記第１の公開鍵復号化手段により復号化された解除鍵を前記第１の公開鍵とは別の第２の公開鍵により暗号化する公開鍵暗号化手段と、前記第２の公開鍵に対応する第２の秘密鍵により前記公開鍵暗号化手段により暗号化された解除鍵を復号化する第２の公開鍵復号化手段とを備えたことを特徴とする請求項１記載の放送信号記録再生装置である。

【００１２】請求項１記載の放送信号記録再生手段は、受信手段が暗号化された放送信号を受信し、解除鍵入力手段が前記放送信号の暗号化を解除する解除鍵を入力し、公開鍵暗号化手段が解除鍵を公開鍵暗号系の公開鍵により暗号化し、記録手段が前記放送信号と暗号化後の解除鍵を記録媒体に記録し、公開鍵復号化手段が記録された暗号化後の前記解除鍵を前記公開鍵と対応する秘密鍵を用いて復号化し、暗号解除手段が記録された前記放送信号の暗号化を解除鍵を用いて解除し、再生・出力手段が暗号解除された放送信号を再生し、出力する。

【００１３】請求項２記載の放送信号記録再生手段では、前記公開鍵暗号化手段が複数の公開鍵を入力し、暗号化された解除鍵を複数生成し、選択手段が記録手段に記録された複数の暗号化後の解除鍵の中から一つの公開鍵に対応する暗号化された解除鍵を選択し、前記公開鍵復号化手段に出力する。

【００１４】請求項３記載の放送信号記録再生手段では、公開鍵暗号化手段が前記公開鍵復号手段により復号化された解除鍵を前記公開鍵とは別の公開鍵により再度暗号化し、公開鍵復号化手段が前記別の公開鍵に対応した秘密鍵により前記再度暗号化された解除鍵を再度復号化し前記暗号解除手段に出力する。

【００１５】

【発明の実施の形態】以下、本発明の実施の形態について、図面を用いて説明する。

【００１６】（実施の形態１）図１は、本発明の請求項１記載の実施の形態の放送信号記録再生装置の構成図であり、同図を参照しながら、本実施の形態の構成を説明する。

【００１７】図１において、本発明の受信手段としての放送受信回路２は、アンテナ１から得られた放送信号を受信し、放送信号を出力する回路手段である。解除鍵入力部３は前記放送信号の暗号を解除する解除鍵を電話等の通信手段を用いて取得するものである。切換回路４ａ、切換回路４ｂはそれぞれ入力データの流れを切り換える回路である。暗号解除回路５は暗号化された放送信号と解除鍵を入力し、復号化した放送信号を出力する回路である。出力回路６は暗号解除回路５からの出力を得てモニタ(図示省略)へ再生信号として出力する手段である。公開鍵入力部７は公開鍵暗号系の公開鍵を入力する手段である。

【００１８】公開鍵暗号化回路８は解除鍵入力部３から解除鍵を入力し、公開鍵入力部７により入力された公開鍵で暗号化する回路である。記録媒体９はデータを記録する手段であり、取りはずすことも可能である。記録部１０は入力されたデータを記録媒体９に記録する。再生部１１は記録媒体９に記録されたデータを読み取る。公開鍵暗号系の公開鍵とその公開鍵に対応する秘密鍵が本発明の放送信号記録再生装置に事前に割り当てられており、秘密鍵記録部１２は機器固有の秘密鍵を保持する手段である。公開鍵復号化回路１３は再生部１１から出力されたデータを入力し、秘密鍵記録部１２の鍵を用いて暗号化された解除鍵を復号化する手段である。

【００１９】以上のような構成において、図１を参照しながら、本実施例の動作を説明する。先ず、リアルタイムで、放送番組を視聴する場合について述べる。

【００２０】図１に示すように、アンテナ１を介して、放送受信回路２により受信された放送信号は、切換回路４ａを介して、暗号解除回路５に送られる。放送の視聴を希望する視聴者は解除鍵入力部３により解除鍵を取得し、切換回路４ｂを介して暗号解除回路５に送る。暗号解除回路５は入力された解除鍵を用いて入力された放送信号の暗号を解除し、出力回路６へ出力する。出力回路６は暗号の解除された放送信号をモニタへ出力する。これにより、視聴を希望する視聴者だけが放送を見ることができる。

【００２１】次に、番組を記録し、それを再生する場合について述べる。

（ステップ１０１）　アンテナ１を介して放送受信回路２により受信された放送信号は記録部１０を介して記録媒体９に記録される。

（ステップ１０２）　放送の視聴を希望する視聴者は解除鍵入力部３により解除鍵を取得する。

（ステップ１０３）　公開鍵入力部７により、視聴者は公開鍵を入力する。このとき、視聴者は記録する放送信号を再生する機器に割り当てられた公開鍵を入力する。即ち、記録する機器と同じ機器で再生する場合は、その機器固有の公開鍵を入力し、記録する機器と再生する機

器が別々の場合は再生する機器固有の公開鍵を入力する。

【００２２】（ステップ１０４）　公開鍵暗号化回路８は解除鍵入力部３により取得された解除鍵を公開鍵入力部７で入力された公開鍵を用いて暗号化し、記録部１０を介して記録媒体９に記録する。

（ステップ１０５）　再生部１１は記録媒体９を読み取り、放送信号を切換回路４ａを介して暗号解除回路５へ出力する。

（ステップ１０６）　再生部１１は暗号化後の解除鍵を公開鍵復号化回路１３に出力する。

（ステップ１０７）　公開鍵復号化回路１３は入力された暗号化後の前記解除鍵を秘密鍵記録部１２に保持されている秘密鍵を用いて復号化し、復号化した解除鍵を切換回路４bを介して暗号解除回路５に出力する。このとき、前記秘密鍵が解除鍵の暗号化に用いられた公開鍵に対応しなければ、元の解除鍵に復号することはできない。

（ステップ１０８）　暗号解除回路５は入力された放送信号を入力された解除鍵を用いて復号化し、出力回路６を介してモニタに出力する。

【００２３】以上のことから、放送信号の解除鍵は、視聴者が選択した機器固有の公開鍵を用いて暗号化した後に記録媒体に記録されるため、その公開鍵と対応する秘密鍵を有する機器のみが解除鍵を復号化でき、放送信号の再生が可能となる。

【００２４】（実施の形態２）図２は、本発明の請求項２記載の実施の形態例の放送信号記録再生装置の構成図であり、図３はデータ構成を説明する図であり、同図を参照しながら、本実施の形態の構成を説明する。

【００２５】図２において、公開鍵リスト入力部２１は複数の公開鍵を取得し、記録する手段である。公開鍵記録部２２は機器固有の秘密鍵に対応する公開鍵を保持する手段である。暗号リスト選択部２３は再生部１１から複数の暗号化された解除鍵リストを入力し、前記公開鍵記録部２２を索引として一つの解除鍵データを選択する手段である。前記以外の構成は実施例１と同じである。

以上のような構成において、図２と図３を参照しながら、本実施例の動作を説明する。リアルタイムで、放送番組を視聴する場合は実施例１と同じである。

【００２６】次に、番組を記録し、それを再生する場合について述べる。

（ステップ２０１）　実施例１の(ステップ１０１)と同じ。

（ステップ２０２）　実施例１の(ステップ１０２)と同じ

（ステップ２０３）　公開鍵リスト入力部２１により、視聴者は記録する放送信号を再生する可能性の有る機器に割り当てられた複数の公開鍵を入力する。

（ステップ２０４）　公開鍵暗号化回路８は解除鍵入力部３により取得された解除鍵を公開鍵リスト入力部２１で入力された公開鍵を用いてそれぞれ暗号化し、暗号化した複数の解除鍵を記録部１０を介して記録媒体９に記録する。図３のデータ構成を用いて説明すると、（ステップ２０３）において、公開鍵３１ａ、公開鍵３１ｂ、公開鍵３１ｃが視聴者により入力された公開鍵であるとすると、それらにより暗号化された解除鍵はそれぞれ暗号化解除鍵データ３２ａ、暗号化解除鍵データ３２ｂ、暗号化解除鍵データ３２ｃとなり、この公開鍵３１ａ、公開鍵３１ｂ、公開鍵３１ｃ、暗号化解除鍵データ３２ａ、暗号化解除鍵データ３２ｂ、暗号化解除鍵データ３２ｃが記録媒体９に記録される。

【００２７】（ステップ２０５）　実施例１の（ステップ１０５）と同じ。

（ステップ２０６）　再生部１１は（ステップ２０４）で記録されたデータリストを暗号リスト選択部２３に出力する。

（ステップ２０７）　暗号リスト選択部２３は複数の暗号化された解除鍵と、公開鍵記録部２２に保持されている公開鍵を用いて、対応する暗号化解除鍵を選択する。図３のデータ構成を用いて説明すると、公開鍵３１ａ、公開鍵３１ｂ、公開鍵３１ｃと公開鍵記録部２２に記録された公開鍵を比較し、同じ公開鍵に対応した暗号化解除鍵を選択し、公開鍵復号化回路１３に出力する。

（ステップ２０８）　実施例１の（ステップ１０７）と同じ。

（ステップ２０９）　実施例１の（ステップ１０８）と同じ。

【００２８】以上のことから、放送信号の解除鍵は、視聴を選択した複数の機器固有の公開鍵を用いて暗号化した後に記録媒体に記録されるため、その複数の公開鍵の中のどれかと対応する秘密鍵を有する機器でのみ再生が可能となる。

【００２９】（実施の形態３）図４は、本発明の請求項３記載の実施の形態の放送信号記録再生装置の構成図であり、同図を参照しながら、本実施の形態の構成を説明する。

【００３０】図４において、認証部４１は公開鍵記録部４２、公開鍵記録部４３が保持している公開鍵に対応する秘密鍵を保持する秘密鍵記録部４３、公開鍵復号化回路４４、公開鍵暗号化回路４５を備えており、本実施例の放送記録再生装置から分離することが可能である。公開鍵記録部２２は（実施例２）と同様に機器固有の公開鍵と秘密鍵を保持する手段である。その他の構成は（実施例１）と同様である。以上のような構成において、図４を参照しながら、本実施例の動作を説明する。リアルタイムで、放送番組を視聴する場合は実施例１と同じである。

【００３１】次に、番組を記録し、それを再生する場合について述べる。

（ステップ３０１）　実施例１の（ステップ１０１）と同じ。

（ステップ３０２）　実施例１の（ステップ１０２）と同じ。

（ステップ３０３）　認証部４１が本実施例の放送記録再生装置に接続されている場合は、公開鍵記録部４２の公開鍵を公開鍵暗号化回路８に出力する。認証部４１が接続されていない場合は、公開鍵暗号化回路８は有効な公開鍵を受け取ることはできない。

【００３２】（ステップ３０４）　実施例１の（ステップ１０４）と同じ。

（ステップ３０５）　実施例１の（ステップ１０５）と同じ。

（ステップ３０６）　再生部１１は暗号化後の解除鍵を公開鍵復号化回路４４に出力する。

（ステップ３０７）　公開鍵復号化回路４４は入力された解除鍵を秘密鍵記録部４３の保持する秘密鍵を用いて復号化し、公開鍵暗号化回路４５に出力する。

【００３３】（ステップ３０８）　公開鍵暗号化回路４５は入力した解除鍵を公開鍵記録部２２の保持する公開鍵で再度暗号化し、公開鍵復号化回路１３に出力する。

（ステップ３０９）　実施例１の（ステップ１０７）と同じ。

（ステップ３１０）　実施例１の（ステップ１０８）と同じ。

【００３４】以上のことから、放送信号の解除鍵は、視聴が有する認証部に保持される公開鍵により暗号化されたのち記録され、記録された解除鍵を復号化するにはその認証部が接続された機器のみが放送信号を再生することが可能となる。

【００３５】

【発明の効果】以上のように本発明によれば、記録媒体が装置から分離可能であっても、有料放送システムにおいて課金された視聴者のみが記録媒体に記録された放送信号を再生できるという長所を有する。

【図面の簡単な説明】

【図１】本発明の実施の形態１の形態による放送信号記録再生装置の構成図

【図２】本発明の実施の形態２の形態による放送信号記録再生装置の構成図

【図３】本発明の実施の形態３の記録媒体に記録される暗号化解除鍵リストのデータ構成を模式的に示した図

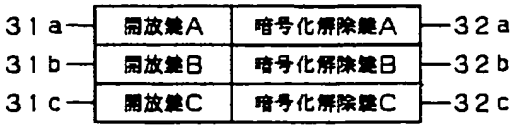
【図４】本発明の実施の形態３による放送信号記録再生装置の構成を示す図

【図５】従来の情報処理装置の構成を示す図

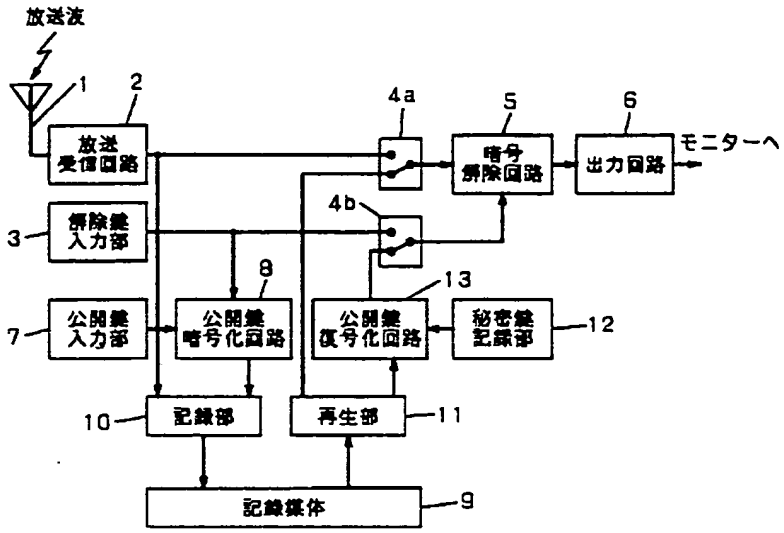
【符号の説明】

１　放送受信回路
２　解除鍵入力部
４ａ　切換回路
４ｂ　切換回路
５　暗号解除回路
６　出力回路
７　公開鍵入力部
８　公開鍵暗号化回路
９　記録媒体
１０　記録部
１１　再生部
１２　秘密鍵記録部
１３　公開鍵復号化回路
２１　公開鍵リスト入力部
２２　公開鍵記録部
２３　暗号リスト選択部
３１ａ　公開鍵Ａ
３１ｂ　公開鍵Ｂ
３１ｃ　公開鍵Ｃ
３２ａ　暗号化解除鍵Ａ
３１ｂ　暗号化解除鍵Ｂ
３１ｃ　暗号化解除鍵Ｃ
４１　認証部

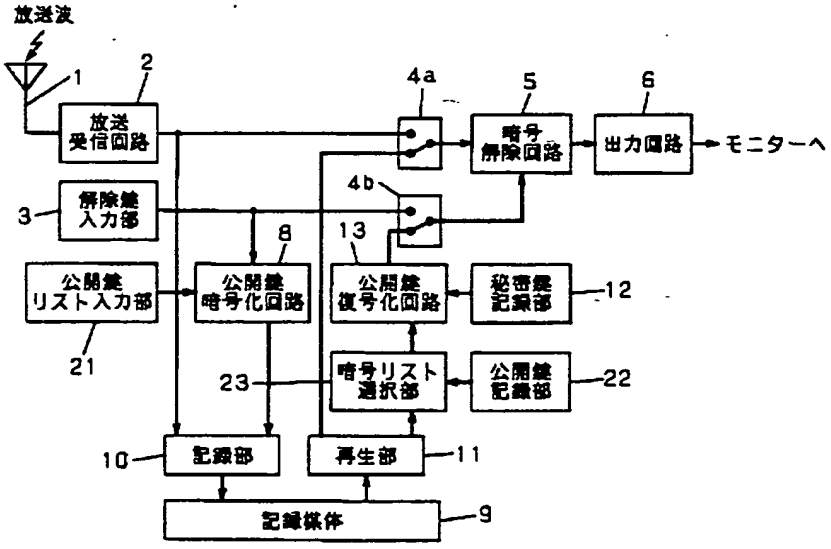
【図３】



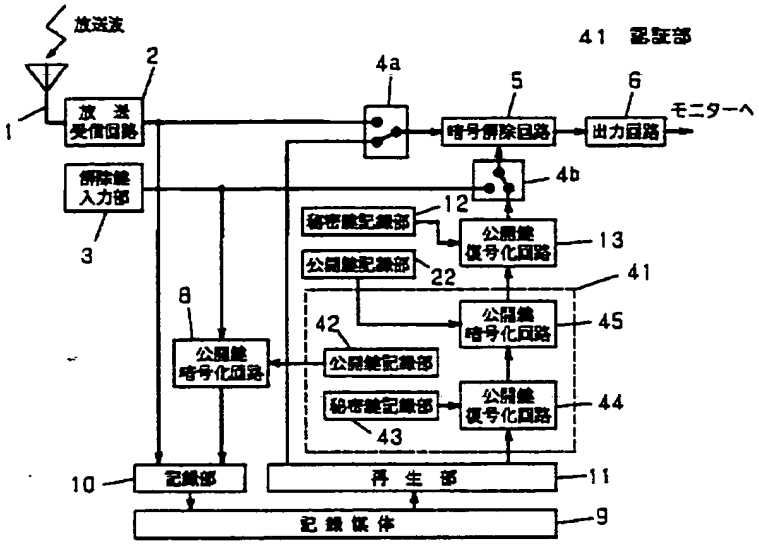
【図１】


放送波
1
2
放送受信回路
4a
5
暗号解除回路
6
出力回路
モニターへ
4b
解除鍵入力部
3
8
13
公開鍵入力部
7
公開鍵暗号化回路
公開鍵復号化回路
秘密鍵記録部
12
10
記録部
再生部
11
記録媒体
9

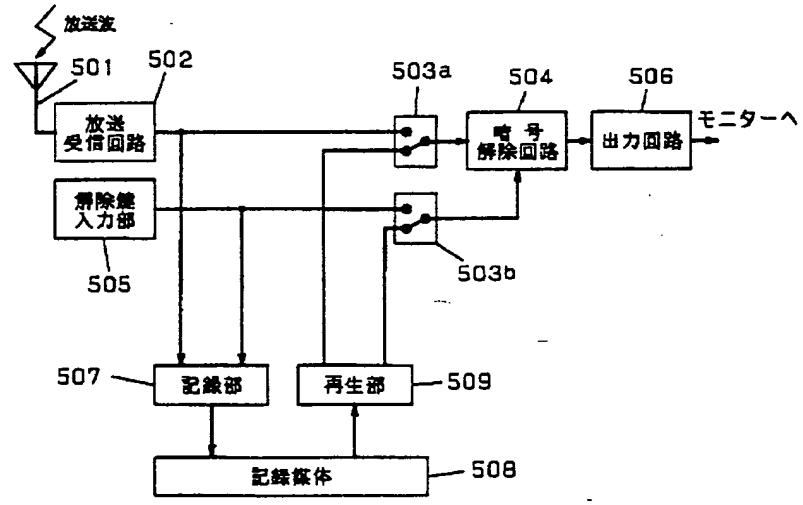
【図２】


放送波
1
2
放送受信回路
4a
5
暗号解除回路
6
出力回路
モニターへ
4b
解除鍵入力部
3
8
13
公開鍵リスト入力部
21
公開鍵暗号化回路
公開鍵復号化回路
秘密鍵記録部
12
23
暗号リスト選択部
公開鍵記録部
22
10
記録部
再生部
11
記録媒体
9

【図４】


放送波
41 認証部
2
4a
5
6
モニターへ
1
放送受信回路
暗号解除回路
出力回路
解除鍵入力部
4b
12
秘密鍵記録部
公開鍵復号化回路
13
公開鍵記録部
22
41
8
公開鍵暗号化回路
42
公開鍵記録部
45
秘密鍵記録部
公開鍵復号化回路
44
43
3
10
記録部
再生部
11
記録媒体
9

【図５】


放送波
501
502
503a
504
506
モニターへ
放送受信回路
暗号解除回路
出力回路
解除鍵入力部
503b
505
507
記録部
再生部
509
記録媒体
508